Sub a7

What is claimed is:

1. A computer program product for enabling a subsequent user sign-on during a certificate-based host access session, said computer program product embodied on a computer-readable medium and comprising:

computer-readable program code means for processing a first sign-on during a secure session using a digital certificate, further comprising:

computer-readable program code means for establishing said secure session from a client machine to a server machine using said digital certificate, wherein said digital certificate represents an identity of said client machine or a user thereof;

computer-readable program code means for storing said digital certificate or a reference thereto at said server machine;

computer-readable program code means for establishing a session from said server machine to a host system using a legacy host communication protocol;

computer-readable program code means for passing said stored digital certificate or said reference from said server machine to a host access security system;

computer-readable program code means, operable in said host access security system, for authenticating said identity using said passed digital certificate or a retrieved certificate which is retrieved using said reference;

computer-readable program code means for using said passed or retrieved digital certificate to locate access credentials for said user;

computer-readable program code means for accessing a stored password or generating a password substitute representing said located credentials; and

computer-readable program code means for using said stored password or said generated password substitute to transparently complete said first sign-on to a secure legacy host application executing at said host system; and

computer-readable program code means for processing a subsequent sign-on during said secure session using said digital certificate, wherein said subsequent sign-on requests access to said secure legacy host application or a different legacy host application, further comprising:

computer-readable program code means for receiving a subsequent sign-on request requiring said identity;

computer-readable program code means for retrieving said stored digital certificate or reference;

computer-readable program code means for passing said retrieved digital certificate or reference from said server machine to said host access security system;

computer-readable program code means, operable in said host access security system, for re-authenticating said identity using said passed retrieved digital certificate or retrieved reference;

computer-readable program code means, operable in said host access security system, for using said passed retrieved digital certificate or retrieved reference to again re-locate said access credentials for said user;

computer-readable program code means for re-accessing said stored password or generating a new password substitute representing said re-located credentials; and

computer-readable program code means for using said re-accessed stored password or said new password substitute to transparently complete said subsequent sign-on to

said secure legacy host application executing at said host system or said different legacy host application.

2. The computer program product as claimed in Claim 1, wherein said digital certificate is an X.509 certificate and said digital certificate reference is a reference to an X.509 certificate.

3. The computer program product as claimed in Claim 1, wherein said communication protocol is a 3270 emulation protocol.

4. The computer program product as claimed in Claim 1, wherein said communication protocol is a 5250 emulation protocol.

5. The computer program product as claimed in Claim 1, wherein said communication protocol is a Virtual Terminal protocol.

6. The computer program product as claimed in Claim 3, wherein said host access security system is a Resource Access Control Facility (RACF) system.

7. The computer program product as claimed in Claim 1, wherein said server machine is a Web application server machine.

8. The computer program product as claimed in Claim 1, further comprising:

computer-readable program code means for requesting by said legacy host application, responsive to said computer-readable program code means for establishing said session, first sign-on information for said user;

computer-readable program code means for responding to said request for first sign-on information by sending a first sign-on message with placeholders from said client machine to said server machine, said placeholders representing a user identification and a password of said user;

computer-readable program code means for substituting a user identifier associated with said located access credentials and said stored password or said generated password substitute for said placeholders in said first sign-on message;

computer-readable program code means for requesting, by said legacy host application, subsequent sign-on information for said user;

computer-readable program code means for responding to said request for subsequent sign-on information by sending a subsequent sign-on message with placeholders from said client machine to said server machine, said placeholders representing said user identification and said password of said user; and

computer-readable program code means for substituting said user identifier associated with said re-located access credentials and said re-accessed stored password or said new password substitute for said placeholders in said subsequent sign-on message.

9. The computer program product as claimed in Claim 7, further comprising:

computer-readable program code means for requesting by said legacy host application,

responsive to said computer-readable program code means for establishing said session, first sign-on information for said user;

computer-readable program code means for responding to said request for first sign-on information by supplying a user identifier associated with said located access credentials and said stored password or said generated password substitute at said server machine;

computer-readable program code means for requesting, by said legacy host application, subsequent sign-on information for said user; and

computer-readable program code means for responding to said request for subsequent sign-on information by supplying said user identifier associated with said re-located access credentials and said re-accessed stored password or said new password substitute at said server machine.

10. A system for enabling a subsequent user sign-on during a certificate-based host access session, comprising:

means for processing a first sign-on during a secure session using a digital certificate, further comprising:

means for establishing said secure session from a client machine to a server machine using said digital certificate, wherein said digital certificate represents an identity of said client machine or a user thereof;

means for storing said digital certificate or a reference thereto at said server machine;

means for establishing a session from said server machine to a host system using a

legacy host communication protocol;

means for passing said stored digital certificate or said reference from said server machine to a host access security system;

means, operable in said host access security system, for authenticating said identity using said passed digital certificate or a retrieved certificate which is retrieved using said reference;

means for using said passed or retrieved digital certificate to locate access credentials for said user;

means for accessing a stored password or generating a password substitute representing said located credentials; and

means for using said stored password or said generated password substitute to transparently complete said first sign-on to a secure legacy host application executing at said host system; and

means for processing a subsequent sign-on during said secure session using said digital certificate, wherein said subsequent sign-on requests access to said secure legacy host application or a different legacy host application, further comprising:

means for receiving a subsequent sign-on request requiring said identity;

means for retrieving said stored digital certificate or reference;

means for passing said retrieved digital certificate or reference from said server machine to said host access security system;

means, operable in said host access security system, for re-authenticating said identity using said passed retrieved digital certificate or retrieved reference;

means, operable in said host access security system, for using said passed retrieved digital certificate or retrieved reference to again re-locate said access credentials for said user;

means for re-accessing said stored password or generating a new password substitute representing said re-located credentials; and

means for using said re-accessed stored password or said new password substitute to transparently complete said subsequent sign-on to said secure legacy host application executing at said host system or said different legacy host application.

11. The system as claimed in Claim 10, wherein said digital certificate is an X.509 certificate and said digital certificate reference is a reference to an X.509 certificate.

12. The system as claimed in Claim 10, wherein said communication protocol is a 3270 emulation protocol.

13. The system as claimed in Claim 12, wherein said host access security system is a Resource Access Control Facility (RACF) system.

14. The system as claimed in Claim 10, wherein said server machine is a Web application server machine.

15. The system as claimed in Claim 10, further comprising:

means for requesting by said legacy host application, responsive to said means for establishing said session, first sign-on information for said user;

means for responding to said request for first sign-on information by sending a first sign-on message with placeholders from said client machine to said server machine, said placeholders representing a user identification and a password of said user;

means for substituting a user identifier associated with said located access credentials and said stored password or said generated password substitute for said placeholders in said first sign-on message;

means for requesting, by said legacy host application, subsequent sign-on information for said user;

means for responding to said request for subsequent sign-on information by sending a subsequent sign-on message with placeholders from said client machine to said server machine, said placeholders representing said user identification and said password of said user; and

means for substituting said user identifier associated with said re-located access credentials and said re-accessed stored password or said new password substitute for said placeholders in said subsequent sign-on message.

16. The system as claimed in Claim 14, further comprising:

means for requesting by said legacy host application, responsive to said means for establishing said session, first sign-on information for said user;

means for responding to said request for first sign-on information by supplying a user identifier associated with said located access credentials and said stored password or said

generated password substitute at said server machine;

means for requesting, by said legacy host application, subsequent sign-on information for said user; and

means for responding to said request for subsequent sign-on information by supplying said user identifier associated with said re-located access credentials and said re-accessed stored password or said new password substitute at said server machine.

17. A method for enabling a subsequent user sign-on during a certificate-based host access session, comprising the steps of:

processing a first sign-on during a secure session using a digital certificate, further comprising the steps of:

establishing said secure session from a client machine to a server machine using said digital certificate, wherein said digital certificate represents an identity of said client machine or a user thereof;

storing said digital certificate or a reference thereto at said server machine;

establishing a session from said server machine to a host system using a legacy host communication protocol;

passing said stored digital certificate or said reference from said server machine to a host access security system;

authenticating, by said host access security system, said identity using said passed digital certificate or a retrieved certificate which is retrieved using said reference;

using said passed or retrieved digital certificate to locate access credentials for

said user;

accessing a stored password or generating a password substitute representing said located credentials; and

using said stored password or said generated password substitute to transparently complete said first sign-on to a secure legacy host application executing at said host system; and

processing a subsequent sign-on during said secure session using said digital certificate, wherein said subsequent sign-on requests access to said secure legacy host application or a different legacy host application, further comprising the steps of:

receiving a subsequent sign-on request requiring said identity;

retrieving said stored digital certificate or reference;

passing said retrieved digital certificate or reference from said server machine to said host access security system;

re-authenticating, by said host access security system, said identity using said passed retrieved digital certificate or retrieved reference;

using, by said host access security system, said passed retrieved digital certificate or retrieved reference to again re-locate said access credentials for said user;

re-accessing said stored password or generating a new password substitute representing said re-located credentials; and

using said re-accessed stored password or said new password substitute to transparently complete said subsequent sign-on to said secure legacy host application executing at said host system or said different legacy host application.

18. The method as claimed in Claim 17, wherein said digital certificate is an X.509 certificate and said digital certificate reference is a reference to an X.509 certificate.

19. The method as claimed in Claim 17, wherein said communication protocol is a 3270 emulation protocol.

20. The method as claimed in Claim 19, wherein said host access security system is a Resource Access Control Facility (RACF) system.

21. The method as claimed in Claim 17, wherein said server machine is a Web application server machine.

22. The method as claimed in Claim 17, further comprising the steps of:

requesting by said legacy host application, responsive to said step of establishing said session, first sign-on information for said user;

responding to said request for first sign-on information by sending a first sign-on message with placeholders from said client machine to said server machine, said placeholders representing a user identification and a password of said user;

substituting a user identifier associated with said located access credentials and said stored password or said generated password substitute for said placeholders in said first sign-on message;

requesting, by said legacy host application, subsequent sign-on information for said user;

responding to said request for subsequent sign-on information by sending a subsequent sign-on message with placeholders from said client machine to said server machine, said placeholders representing said user identification and said password of said user; and

substituting said user identifier associated with said re-located access credentials and said re-accessed stored password or said new password substitute for said placeholders in said subsequent sign-on message.

23. The method as claimed in Claim 21, further comprising the steps of:

requesting by said legacy host application, responsive to said step of establishing said session, first sign-on information for said user;

responding to said request for first sign-on information by supplying a user identifier associated with said located access credentials and said stored password or said generated password substitute at said server machine;

requesting, by said legacy host application, subsequent sign-on information for said user; and

responding to said request for subsequent sign-on information by supplying said user identifier associated with said re-located access credentials and said re-accessed stored password or said new password substitute at said server machine.